METHOD AND APPARATUS FOR SECURED SOCIAL NETWORKING

TECHNICAL FIELD

[0001] Embodiments of the present invention relate generally to communication technology, and, more particularly, relate to a method and apparatus for secured pervasive social networking based on multi-dimensional trust levels.

BACKGROUND

[0002] A mobile ad hoc network (MANET) may be configured for use as a platform for a social group when performing social networking activities, e.g., for so called Pervasive Social Networking. A MANET is defined as a collection of autonomous nodes that are configured to communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. A social group may be instantly formed not only by people socially connected, but those persons that are physically in proximity, such as groups for purchase, resource sharing and social events. For example, a person may chat with nearby stranger for instant social needs (e.g. responding to group purchase activities, ride sharing and/or music preferences). This kind of pervasive social networking may be valuable to a mobile user especially if mobile Internet or other wireless networks are unavailable or are costly to access. MANET based instant social networking could be valuable for preserving user privacy and perhaps more than traditional social networking sites.

SUMMARY

[0003] Methods, apparatuses, and computer program products are herein provided for controlling access of communications in a Pervasive Social Network (PSN) using a local trust level and/or a general trust level. In some example embodiments, a user operating a communication device on a PSN may select other users with at least a minimum level of local and/or general trust for secure communications. For example, users having a communication device (e.g., a mobile device) with a trust level lower than the minimum level of trust would not be configured to access the secure communications.

[0004] In some example embodiments and in an instance in which a trusted server is available, a user may control access to secure communications based on a general trust level that is evaluated by the trusted server. In some example embodiments, the secure communication access based on the general trust level may be controlled by keys (e.g., an encryption public key and one or more personalized decryption keys) that are generated and issued by the trusted server.

[0005] In other example embodiments, the user may control communication data access based on both a general trust level and a local trust level. For example, based on periodically issued keys from the server and locally generated keys, the user may further control the access of its secure communications by encrypting its messages using both the key issued by the server corresponding to the general trust level and the key generated by its local device corresponding to the local trust level. The user may then broadcast encrypted messages to nearby communication devices that may be decrypted using the personalized secret keys issued by both the trusted server and the user device that encrypts the message.

[0006] Alternatively or additionally, in an instance in which the server is not available, each user having a communication device on the PSN may generate an encryption key and corresponding personalized secret keys based on a determined local trust level for encryption and decryption of PSN communication data. The user communication device is configured to evaluate the current local trust levels of other communication devices and set the communication data access policy for itself. The user may then issue the keys to those users that satisfy the decryption conditions (e.g., data access conditions, concretely meet or satisfy an expected local trust level). The user may then broadcast encrypted messages to nearby communication devices that may be decrypted using the issued keys.

[0007] In one embodiment, a method is provided that comprises determining a general trust level for one or more users. The method of this embodiment may also include generating a public encryption key and one or more personalized decryption secret keys for the one or more users based on the general trust levels of the one or more users. The method of this embodiment may also include causing the public encryption key and the one or more personalized decryption secret keys to be issued to the one or more users. In some example embodiments, the one or more users are configured to encrypt a message based on the public encryption key. In some example embodiments, the one or more users are configured to decrypt the message using the corresponding personalized secret decryption keys if the access control conditions are satisfied (e.g., its general trust level satisfies an expected level).

[0008] In another embodiment, an apparatus is provided that includes at least one processor and at least one memory including computer program code with the at least one memory and the computer program code being configured, with the at least one processor, to cause the apparatus to at least determine a general trust level for one or more users. The at least one memory and computer program code may also be configured to, with the at least one processor, cause the apparatus to generate a public encryption key and one or more personalized decryption secret keys for the one or more users based on the general trust levels of the one or more users. The at least one memory and computer program code may also be configured to, with the at least one processor, cause the apparatus to cause the public encryption key and the personalized decryption secret keys to be issued to the one or more users. In some example embodiments, the one or more users are configured to encrypt a message based on the public encryption key. In some example embodiments, the one or more users are configured to decrypt the message using one or more corresponding personalized secret decryption keys if the access control conditions are satisfied (e.g., its general trust level satisfies an expected level).

[0009] In a further embodiment, a computer program product may be provided that includes at least one non-transitory computer-readable storage medium having computer-readable program instructions stored therein with the computer-readable program instructions including program instructions configured to determine a general trust level for one or more users. The computer-readable program instructions may also include program instructions configured to generate a public encryption key and one or more personalized decryption secret keys for the one or more users based on the general trust levels of the one or more users. The computer-readable program instructions may also include program instructions